IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA v. MOHAMMED AZHARUDDIN CHHIPA, Defendant.	Case No. 1:23-CR-97 Hon. David J. Novak

GOVERNMENT'S RESPONSE IN OPPOSITION TO DEFENDANT'S MOTIONS TO SUPPRESS THE UNLAWFUL SEARCH OF HIS INTERNET SERVICE ACCOUNTS

Defendant moves to suppress the contents of two voluntary emergency disclosures made by Facebook, one on March 20, 2019, and another on August 1, 2019, in response to requests made by the Federal Bureau of Investigation ("FBI") pursuant to the Stored Communications Act ("SCA"), 18 U.S.C. § 2702(b)(8).[1] In March of 2019, in the wake of the Christchurch, New Zealand massacre and after having posted little for years, the defendant suddenly posted a stream of violent, threatening, pro-ISIS content, creating a good faith belief that an emergency involving danger of death or serious physical injury required disclosure without delay. Then again, in August of 2019, after the defendant sent money to a woman in the Philippines who was subsequently arrested for terrorism-related offenses, the FBI applied for another voluntary

[1] The defense timely filed a motion to suppress the contents of the March 20, 2019 voluntary disclosure from Facebook on September 20, 2024. *See* Dkt. No. 156. Shortly thereafter, the government became aware of a second disclosure made by Facebook in response to a voluntary disclosure request pursuant to 18 U.S.C. § 2702(b)(8) issued on August 1, 2019. On September 26, 2024, the government disclosed the fact of the second request and disclosure, as well as the substance of what the FBI submitted to Facebook in its request. On September 30, 2024, the government provided Facebook's response to the request (i.e., the account information) to the defense. Also on September 30, 2024, defense filed a second motion to suppress for the August 1, 2019 voluntary disclosure from Facebook. Dkt. No. 164. The fault was the government's, and the government does not object on timeliness to the defense's second motion to suppress.

disclosure from Facebook, fearing that the defendant might react in a desperate fashion following the arrest of his co-conspirator.

In each instance, the FBI acted in good faith reliance on the statute as written and with a reasonable belief that exigent circumstances justified proceeding without a warrant. Furthermore, the FBI would have inevitably discovered the material via search warrant regardless of the § 2702 disclosures. Accordingly, the defendant's motion should be denied.

BACKGROUND

In March of 2019, the FBI's investigation into the defendant was closed. The defendant had previously been investigated after telling officials at the U.S.-Canadian border that he was interested in traveling overseas to fight with his Muslim brothers and kill Americans. See Ex. 1 (FBI 302 dated March 28, 2019) at 3 (under seal). He was also known to have posted pro-Al Qaeda propaganda on his social media. See *id*. at 6. From January 2015 to February 2019, however, the defendant's Facebook account, the Carl Johnson account, "lay dormant." *Id*. It was during this time period that the FBI's Washington Field Office ("WFO") closed its investigation.

On March 15, 2019, an FBI agent in Miami, Special Agent Waldron, was monitoring a Facebook community page known to espouse support for the Foreign Terrorist Organization ISIS, also known as the Islamic State of Iraq and al-Sham. See Ex. 2 (FBI 302 dated March 27, 2019) at 4 (under seal). SA Waldron noticed the Carl Johnson account "lik[ing] numerous concerning posts." *Id.* SA Waldron then viewed the publicly available data on the Carl Johnson Facebook page and observed multiple, recent "posts supportive of violent jihad and clerics who are supportive of ISIS and radical Islam." *Id.* at 4. The posts on the Carl Johnson page included pictures of apparent jihadi soldiers holding weapons, captions like, "The sword is a must. Jihad is a must. Nothing terrifies . . . the enemies of the Muslimin . . . like power, force, and weapons,"

and pictures of green birds (a known reference to martyrdom in the online jihadi community). *Id*.; *see*, *e.g.*, "Nashid Album Cover," Combating Terrorism Center at West Point, available at https://ctc.westpoint.edu/militant-imagery-project/0251/ (discussing jihadi visual motifs regarding martyrs generally, and noting that "the souls of martyrs are believed to live in the crops of green birds.")

The Miami field office checked FBI holdings to see if there was any additional information on this highly concerning account. They discovered it was linked to Mohammed Chhipa through the then-closed investigation. On March 18, 2019, FBI Miami contacted FBI WFO "to advise of the recent re-emergence of Chhipa on Facebook and his disturbing posts/likes/comments indicating an allegiance to ISIS and a possible desire to conduct violent jihad." *See* Ex. 2 at 6.

WFO was not receiving this information in a vacuum. At that time, the horrific Christchurch mosque shooting had just occurred in New Zealand on March 15, 2019, and FBI was concerned for copycat attacks against mosques in the United States, or for terror plots by Islamic extremists seeking revenge. *See, e.g.*, '"We will never live in fear:' US mosques on high alert after New Zealand attack," The Guardian (Mar. 15, 2019), available at https://www.theguardian.com/us-news/2019/mar/15/us-mosques-high-alert-new-zealand-shooting-prayer (noting ramped up police presence at local mosques in major US cities); Department of Justice Press Release, San Fernando Valley Man Found Guilty in Terror Plot to Bomb a Rally in Long Beach, available at https://www.justice.gov/opa/pr/san-fernando-valley-man-found-guilty-terror-plot-bomb-rally-long-beach (noting that "[f]ollowing an attack on Muslims in New Zealand in March 2019, Domingo called for retribution in an online post"); Ex. 1 at 6 (noting that "*[i]n the wake of the New Zealand mosque attacks on March 15, 2019*, Chhipa

posted 'The sword is a must. Jjihad is a must. Nothing terrifies the enemies … of the Muslimin …like power, force, and weapons.'") (emphasis added). Now, amid this tense environment, someone who had previously expressed interest in fighting overseas with his Muslim brothers and killing Americans was suddenly posting a stream of pro-ISIS, violent content, after a lengthy period of little activity on his account.

As a result, the very next day, on March 19, 2019, FBI WFO requested a § 2702 emergency disclosure related to the Carl Johnson Facebook account. Ex. 3 (FBI 302 summarizing Carl Johnson 2702 request) (under seal). As provided by the statutory framework, this request was for voluntary disclosure, with Facebook making the ultimate call of whether to turn over material to the FBI. Facebook, which had the opportunity to review the full contents of the account before deciding whether to comply, decided that the situation merited disclosure without delay, and provided the account contents for a limited, recent time period on March 20, 2019.[2] The production revealed additional pro-ISIS, dangerous content, including the defendant stating in a private message, "I've already planted the seeds and realized that I only have 3-4 destinations in life and I accept whatever Allah Aza Wajjal will give me: …prison, *hijrah/jihaad* (migration/fighting), s*hahadah* (martyrdom)." Ex. 1 at 4.

The investigation into the defendant was re-opened. Using primarily grand jury subpoenas and an online covert employee (OCE), the FBI identified numerous other Facebook accounts used by the defendant, including the Nu'man Ibn Muqrin Al-Muzanee account (hereafter, the Al-Muzanee account). *See* Ex. 4 (Search Warrant for Nine Facebook Accounts, August 8, 2019), Affidavit at 4—12 (under seal). In June of 2019, the OCE asked the defendant if he was "planning for *qital* [killing/slaying]," to which the defendant responded, "*Na'am akhee*

[2] The date range for the account production was February 1, 2019 through March 19, 2019. Thus, Facebook only produced a small portion of the content for this account. The account was registered on June 6, 2008.

in sha Allah [yes my brother if God wills it]." The OCE asked "U going to do operation then…?" and the defendant responded, "*Na'am* [yes] we will see what happens *in sha Allaah* [if God wills it] in this next couple of months." *See* Ex. 5 at 6 (OCE-3 interactions … from 14 through 22 June 2019) (under seal).

In addition to the defendant's concerning social media posts and conversations with the OCE, the FBI also identified thousands of dollars in financial transactions between March and July 2019, from the defendant to a specific, Philippines-based individual. *See* Ex. 6 (search warrant for 4036 Pender Ridge Terrace, Fairfax, Virginia), Affidavit at 9—13 (under seal). That individual was arrested by Filipino law enforcement on July 24, 2019. Her arrest was covered in the Filipino news media, identifying her as affiliated with Dawlah Islamiyah Turaife Group (the Islamic State Turaife Group), an ISIS-inspired group believed responsible for at least three terrorist bombings since August of 2018. *See, e.g.*, "2 Alleged ISIS Sympathizers Nabbed in GenSan Raid," Philippine News Agency (July 24, 2019), available at https://www.pna.gov.ph/articles/1075901. The articles stated that she would be charged with illegal possession of firearms, ammunition, explosives, and allegedly purchasing bomb-making materials for the Turaife Group. *See id.*

Based on the defendant having previously said that he only saw three paths for himself in life (prison, hijrah/jihaad, and martyrdom), his stated interest in killing/slaying "in this next couple of months," and the arrest of his co-conspirator in the Philippines, the FBI assessed there was an emergency situation and asked Facebook to voluntary produce records for the Al Muzanee Facebook account. *See* Ex. 7 (FBI 302 summarizing Aug. 1 request to Facebook for voluntary disclosure of records) (under seal). Facebook agreed that there was a good faith belief that an emergency involving danger of death or serious physical injury required disclosure

without delay, and provided recent content of the account that same day.[3] The disclosure revealed the defendant telling an associate in the Philippines of the need "to keep everything as secretive as possible." *See* Ex. 6, Affidavit at 12. The associate told Chhipa: "they've been tracing u here since u are involved in sending money," that he should not "use [his] identity or [his] name for sending money," and that "tomorrow some FBI will go to our country to investigate…theyre asking about u and the authorities here." *Id.* at 12—13. Chhipa told the associate that the people around him, like his family, were scared and would not help him. *Id.* at 13. The disclosure also revealed that Chhipa would not hesitate to destroy evidence if he believed the FBI were close to arresting him. In a May 15, 2019, conversation, the defendant described "the FBI was going around with my pictures," and how he almost "destroy[ed] my computer…like hard drives and stuff." *Id.* at 14—15.

On August 2, 2019, the FBI obtained a search warrant for the defendant's home. On August 8, 2019, the FBI obtained a search warrant for the Carl Johnson account, the Al Muzanee Facebook account, and seven others operated by the defendant under aliases. Facebook generated the warrant responses on or about August 11, 2019 at 23:07 UTC (approximately three days after the issuance of the warrants). In the days following the execution of the warrant at the defendant's home, the defendant eluded FBI surveillance and fled the country.

ARGUMENT

The government does not challenge the overall presumption that individuals generally have a reasonable expectation of privacy in the content of their private communications when using a third-party service like Facebook. There is little guidance for how this general principle should be assessed in the context of the voluntary emergency disclosures at issue in this case,

[3] The date range for Facebook's production was May 4, 2019, through August 1, 2019. This was a new account, registered on May 4, 2019.

where Facebook made the determination of whether to disclose anything at all and then what to disclose, and where Facebook has strong independent reasons for preventing its platform from being used for the promotion or planning of acts of terrorism and violence.[4] The government respectfully suggests that it is not necessary for the Court to decide this question, however, since the defendant's motion can be resolved based on the exigent circumstances exception, good faith reliance on the statutory provisions contained in 18 U.S.C. § 2702(b)(8), and inevitable discovery based on the subsequent warrants executed for the accounts.

A. Exigent circumstances led the FBI to seek the voluntary disclosure.

"As the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is 'reasonableness.'" *Maryland v. King*, 569 U.S. 435, 447 1969 (2013) (citation omitted). Because of this, a "warrant is not required to establish the reasonableness of *all* government searches," *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995), and the Supreme Court has recognized certain exceptions to the warrant requirement. Exigent circumstances is a well-established exception that can render a warrantless search constitutionally reasonable. This exception applies when '"the exigencies of the situation' make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment." *Mincey v. Arizona*, 437 U.S. 385, 393-94 (1978). *See also Mora v. The City of Gaithersburg, MD*, 519 F.3d 216, 222 (4th Cir. 2008) (stating that the assessment of Fourth Amendment reasonableness requires "pragmatism" and noting that "[i]f there is a grave public need for the police to take preventive action, the Constitution may impose limits,

[4] *Cf. United States v. Chatrie*, 107 F.4th 319, 331–32 (4th Cir. 2024) (distinguishing Carpenter and finding that third-party doctrine governed and government acquisition of location history from Google was not a Fourth Amendment search because "unlike with CSLI, a user knowingly and voluntarily exposes his Location History data to Google," and location history is not "'such a pervasive and insistent part of daily life' that [activating it] is indispensable to participation in modern society.").

but it will not bar the way."); *see also United States v. Laudermilt*, 677 F.3d 605, 611 (4th Cir. 2012) (quoting Mora and reversing district court determination that exigent circumstances exception did not justify sweep of entire house after defendant was arrested and secured).

The categories of "emergency conditions" that generally support the application of the exigent circumstances doctrine are: "(1) the need to pursue a fleeing suspect; (2) the need to protect individuals who are threatened with imminent harm; and (3) the need to prevent the imminent destruction of evidence." *United States v. Hobbs*, 24 F.4th 965, 969-70 (4th Cir. 2022), *cert. denied*, 142 S.Ct. 2825 (2022). Courts evaluate the totality of the circumstances to determine whether an emergency is "enveloped by a sufficient level of urgency" to be reasonable under the Fourth Amendment, in light of "officers' objectively reasonable belief based on specific articulable facts and reasonable inferences that could have been drawn" from those facts. *Id*. at 970 (internal citations and quotations omitted).

This Circuit has addressed exigent circumstances in the context of the emergency disclosure of location information. In *Hobbs*, the Fourth Circuit held that exigent circumstances permitted the warrantless collection of prospective location information and call logs pursuant to an emergency request to defendant's cell phone provider where a defendant with a violent criminal history had recently brandished a firearm to his former girlfriend and then forcibly entered her home and removed a television. *Id.* at 970—71. Before leaving the home, he had threatened to harm his former girlfriend and her family members and any responding officers if she contacted police. *Id*. The court found that these facts, in addition to information that the defendant's "cell phone provider was known to be 'notoriously slow' in responding to law enforcement search warrants and could take several days to produce the necessary cell phone location information" made it reasonable for officers to conclude that exigent circumstances

supported the warrantless acquisition of location information by an emergency request. *Id*. at 971. Similarly, in *United States v. Karmo*, the Seventh Circuit found that exigent circumstances justified the warrantless collection of real time cell site location information (without deciding whether a Fourth Amendment search occurred) where defendant was traveling with firearms to Kenosha, Wisconsin, during a period of civil unrest. *United States v. Karmo*, 109 F.4th 991, 995 (7th Cir. 2024) ("Exigent circumstances are present if law enforcement reasonably believes that the safety of the public is threatened,"); *see also United States v. Gilliam*, 842 F.3d 801, 804 (2d Cir. 2016) (finding exigent circumstances justified tracking defendant's phone where he was trafficking a minor for work as a prostitute); *United States v. Torres*, 661 F. Supp. 3d 1098, 1102–03 (D.N.M. 2023) (in parental kidnapping case, finding that government acquisition of three days of GPS and other location information for six phone numbers and two email addresses used by the defendant was objectively reasonable and fell within exigent circumstances exception). The Fourth Circuit also addressed the exigent circumstances justification for warrantless searches in the "preventive action" context in *Mora,* 519 F.3d at 226, holding that the warrantless search of a suspect's luggage, van, and apartment was constitutionally permissible in light of a hotline tip that the suspect planned to commit mass murder. In describing the balancing of interests that underpins the assessment of whether exigent circumstances justify a particular warrantless search or seizure, the court in *Mora* emphasized "[a]s the likelihood, urgency, and magnitude of a threat increase, so does the justification for and scope of police preventive action. In circumstances that suggest a grave threat and true emergency, law enforcement is entitled to take whatever preventive action is needed to defuse it." *Id*. at 224-25.

While it is inherently difficult to assess the likelihood that an individual who has expressed an interest in committing or supporting acts of terror might carry out those acts, the

magnitude of the threat — potentially involving mass casualties — is at the highest possible level. The government's compelling interest in preventing violent terrorist acts should weigh heavily on the government's side in balancing the interests at stake to assess the reasonableness of the government's belief that the circumstances justified proceeding under the emergency provisions of the SCA. The defendant had long been a person of concern to the FBI. He had threatened to travel overseas to fight with his Muslim brothers, expressed a desire to kill Americans, voiced support for Al Qaeda, and written online that he hoped to die a *shaheed* (martyr). Then, after years of quiet and in the highly charged environment following the Christchurch shooting, his account reappeared, posting and liking a high volume of extreme content in support of ISIS, jihad, and acts of violence. *See* Ex. 2. His Facebook activity included: posting a picture of armed militants with the words "[t]he sword is a must. Jihad is a must. Nothing terrifies the enemies…like power, force, and weapons," liking a post stating, "[y]ou attacked our Islamic State," multiple posts featuring firearms, posts featuring the ISIS flag, posts supportive of martyrdom, and others. The posts were threatening enough that the FBI Miami agent, who was monitoring a Facebook community page where users espouse support for ISIS, honed in on the Carl Johnson account. The agent quickly researched the account both online and in FBI systems and relayed the information to WFO.

It's difficult to overstate the dangerousness of the FTO, ISIS, at issue in this case. As the FBI Director stated in remarks to the U.S. Senate in 2019, "ISIS remains relentless and ruthless in its campaign of violence against the West and has aggressively promoted its hateful message, attracting like-minded violent extremists." Christopher Wray, Statement Before the Senate Homeland Security and Governmental Affairs Committee (Nov. 5, 2019), available at: https://www.fbi.gov/news/testimony/worldwide-threats-110519. In the two years prior to the

defendant's posts (calendar years 2017 and 2018), ISIS had been linked to over 50 terrorist incidents worldwide, resulting in the death of thousands of people. *See List of Terrorist Incidents Linked to the Islamic State*, Wikipedia, available at: https://en.wikipedia.org/wiki/List_of_terrorist_incidents_linked_to_the_Islamic_State. ISIS also had been specifically linked to several attacks in the United States. *Id.*

WFO, recognizing the exigent circumstances, acted with the appropriate speed. They received the information on March 18, 2019, and applied for the voluntary disclosure the next day on March 19, 2019. At the time that they sought emergency disclosure from Facebook, law enforcement reasonably believed that the gravity of the threat of violent terrorist acts potentially committed or supported by the account holder justified proceeding under the SCA's emergency provisions without a warrant.[5] The defendant was posting in support of violence and a foreign terrorist organization. These posts indicated that he was aware that ISIS is an organization that engages in terrorist activity, and that he desired to personally support the organization and acts of violence. He was also publicly active on other Facebook pages seeking out other like-minded individuals.

Facebook, which had access to the defendant's entire profile, determined that there was a good faith belief that an emergency involving danger of death or serious physical injury required disclosure without delay. *See* 18 U.S.C. § 2702(b)(8) ("A provider … *may* divulge the contents of a communication … if *the provider*, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay…") (emphasis added); *see also* Meta Transparency Center, Further Asked Questions, available at

[5] In addition, although probable cause is not required for exigent circumstances to justify a warrantless search to prevent injury or harm to the public, law enforcement had probable cause to believe that the account contained evidence of criminal activity including support for terrorism.

https://transparency.meta.com/reports/government-data-requests/further-asked-questions/ (noting that Meta "may voluntarily disclose" in response to an emergency disclosure based on the circumstances, and that Meta does "push back on or challenge a request" if it is not consistent with applicable law or their policies). Facebook voluntarily provided the communications on March 20, 2019, which revealed additional concerning posts and messages, including that the defendant had "already planted the seeds" and was prepared for prison, traveling overseas and fighting ("hijrah/jihaad"), or martyrdom. Facebook would also have been able to see the defendant discussing suspicious international transfers of money, including the defendant stating, "I can't send from my bank account for a number of reasons." *See* Ex. 6, Affidavit at 9.

In August of 2019, there again existed exigent circumstances. The defendant, who had by now repeatedly expressed interest in killing, sent thousands of dollars to a woman publicly linked to purchasing bomb-making materials for an ISIS affiliated group. Following her arrest, the FBI acted out of a good faith concern for how the defendant would react following the arrest of a co-conspirator. His communications could reasonably be expected to indicate whether he was engaged in an ongoing conspiracy to send money to the Philippines to fund a potential terror attack, or if he was plotting to take action here in the United States in light of the frustration or discovery of his money remitting scheme to the Philippines.

Finally, it is worth noting that in the midst of these fraught situations, the FBI received the recent content of the accounts faster than it otherwise would have by using emergency disclosure requests, allowing them to more quickly assess the risk to the public posed by the defendant. Facebook typically responds faster to emergency disclosure requests than to traditional warrants. In this case, Facebook provided the March voluntary disclosure within a day, the August voluntary disclosure the same day, but took three days to respond to the warrant

on August 8, 2019, for the content of the accounts. And three days is the fastest that Facebook has responded to a warrant in this case. When the government obtained another search warrant for one Facebook and one Instagram account on October 22, 2020 (1:20-sw-1559), Facebook didn't generate the report until November 20, 2020, nearly a full month later. When the government obtained for a search warrant for three Facebook accounts and eight Instagram accounts on June 6, 2022 (1:22-sw-326), Facebook didn't generate a response until June 28, 2022. *See Hobbs*, 24 F.4th at 971 (finding that cell phone company potentially taking "several days" to produce location information in response to a warrant increased risk of harm and supported warrantless collection of location information).

Under these circumstances, the government's emergency acquisition of recent contents of the defendant's accounts was objectively reasonable and fell within the exigent circumstances exception to the warrant requirement.

B. Law enforcement relied in good faith on the statute as written for a voluntary production of records.

Even if the Court finds that the exigent circumstances exception does not apply and that a search warrant was required, the government respectfully submits that exclusion is not the appropriate remedy because the government relied in good faith on the emergency provisions of the SCA.

Suppression is a remedy of last resort, to be used for the sole purpose of deterring future Fourth Amendment violations and only when the deterrence benefits of suppression outweigh its heavy costs. *Davis v. United States*, 564 U.S. 229, 236-37 (2011); *United States v. Perez*, 393 F.3d 457, 460 (4th Cir. 2004). Accordingly, suppression of evidence is appropriate only when law enforcement conduct is "sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Herring*

v. United States, 555 U.S. 135, 144 (2009); *see also United States v. Peltier*, 422 U.S. 531, 542 (1975) (evidence should be suppressed "only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment."). The good faith exception applies to searches conducted in reasonable reliance on statutory provisions even if they are later invalidated, because "[t]he application of the exclusionary rule to suppress evidence obtained by an officer acting in objectively reasonable reliance on a statute would have as little deterrent effect on the officer's actions as would the exclusion of evidence when an officer acts in objectively reasonable reliance on a warrant." *Illinois v. Krull*, 480 U.S. 340, 349 (1987). As previously discussed, the agents had a good faith belief that the situation merited immediate disclosure, and they reasonably relied on the provisions of 18 U.S.C. § 2702(c)(8).

Defendant suggests that the emergency provisions of § 2702 were invalidated or undermined by *Carpenter v. United States*, 585 U.S. 296 (2018), in which the Supreme Court ruled that the compelled disclosure of comprehensive cell site information is a Fourth Amendment search that generally requires a search warrant rather than a court order under 18 U.S.C. § 2703(d). *Carpenter* cannot be read as silently rendering Section 2702(b)(8) unconstitutional. The Court in *Carpenter* emphasized that the decision was "a narrow one." *Id.* at 298. In fact, the Court explicitly recognized that "case-specific exceptions" including "urgent situation[s]" can still support the warrantless search of an individual's cell-site records and further explained that the "decision today does not call into doubt warrantless access to CSLI in such circumstances. While police must get a warrant when collecting CSLI to assist in the mine-run criminal investigation, the rule we set forth does not limit their ability to respond to an ongoing emergency." *Id.* at 2222. *See also Hobbs*, 24 F.4th at 971 n.3 (noting that *Carpenter* did

not express an opinion regarding "real-time" location information or the use of such data under exigent circumstances); *Torres*, 661 F. Supp. 3d at 1103 (stating that *Carpenter* "supports" the emergency disclosure of location information by cellphone provider).

Here, the FBI relied on a provision of the SCA that has not been invalidated and that relies on voluntary disclosure in an emergency situation.[6] Neither *Carpenter* nor any other controlling authority precludes the government from requesting and obtaining a voluntary disclosure from a social media company under the circumstances outlined in § 2702(b)(8) or makes it unreasonable to rely on that provision of the SCA. Even where a provision of the SCA was later invalidated, the Fourth Circuit has recognized that officers were entitled to rely on the SCA's statutory provisions for the warrantless acquisition of cell site location information prior to *Carpenter*. *United States v. Chavez*, 894 F.3d 593, 608 (4th Cir. 2018) (noting that "[w]hile *Carpenter* is obviously controlling going forward, it can have no effect on Chavez's case" because reasonable reliance on the subsequently invalidated portion of the SCA established "'objectively reasonable good faith.").

While much of the litigation regarding the SCA's emergency provisions involves the disclosure of location information, at least one court has explicitly found the officer's good faith reliance on § 2702(b)(8) makes suppression inappropriate. In *United States v. Duncan*, the FBI applied for and obtained emergency disclosure of the defendant's Instagram account when his wife reported in October of 2020 his "suspected involvement in firearm and explosives manufacturing," and text messages obtained by warrant "indicated prior conversations on Instagram contextualizing the violent plans that concerned her." *United States v. Duncan*, 2024

[6] *See also* Facebook Terms of Service (Sept. 9, 2016 version), available at: https://www.facebook.com/privacy/policy/version/20160929/ (noting that they may "access, preserve and share information when we have a good faith belief it is necessary to … protect . . . others or to prevent death or imminent bodily harm.").

WL 331890, at *1 (E.D. N.C. Jan. 29, 2024). The Court upheld the disclosure because the officers relied in good faith on the voluntary disclosure of Duncan's direct messages to respond to an emergency. In so finding, the Court noted the lack of "any precedent holding that § 2702 is unconstitutional on its face or as applied to the circumstances presented in this case." *Id*. at *3. The court went on to state, "applying the Fourth Amendment to social media accounts is a relatively unexplored area of law with nuances that have yet to be discovered. Courts should not punish law enforcement officers who are on the frontiers of new technology simply because 'they are at the beginning of a learning curve and have not yet been apprised of the preferences of courts on novel questions.'" *Id*. To the extent reliance on the SCA's emergency provisions under these circumstances is unsettled, the Fourth Circuit also has recognized, "[i]t is axiomatic that courts should not punish law enforcement officers who are on the frontiers of new technology simply because they are at the beginning of a learning curve and have not yet been apprised of the preferences of courts on novel questions." *Zelaya-Veliz*, 94 F.4th 321, 341 (4th Cir. 2024) (citations and quotations omitted). Law enforcement "cannot be expected to question the judgment of the legislature that passed the law[s]" providing for emergency disclosure under the SCA, *Krull*, 480 U.S. at 350, and justifiably relied in good faith on the emergency disclosure provisions of 18 U.S.C. § 2702(b)(8).

The circumstances of this case do not support a finding of "deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights" that would make the deterrent value of excluding evidence sufficiently strong to outweigh the costs to the justice system. *United States v. Qazah*, 810 F.3d 879, 887 (4th Cir. 2015) (citing *Davis,* 131 S.Ct. 2419 at 2422). To the contrary, the circumstances here demonstrate that investigators relied in good faith on statutory provisions in light of their belief that the defendant posed an imminent threat of great harm by

supporting a brutally violent foreign terrorist organization. Investigators thus acted with "'an objectively reasonable good-faith belief that their conduct is lawful . . . and exclusion cannot pay its way.'" *Id*. (quoting *Davis,* 131 S.Ct. 2419 at 2422).

C. The inevitable discovery doctrine further supports that suppression is not warranted.

The inevitable-discovery doctrine allows the government to use information obtained from an otherwise unreasonable search if it can establish by a preponderance of the evidence that law enforcement would have "ultimately or inevitably" discovered the evidence by "lawful means." *Nix v. Williams*, 467 U.S.431, 444 (1984); *United States v. Bullette*, 854 F.3d 261, 265 (4th Cir. 2017). To establish that officers inevitably would have discovered the challenged evidence by lawful means, the government must meet two criteria: first, that it had, or would have obtained, an independent, legal justification for conducting a search that would have led to the discovery of the evidence; and second, that it would have conducted a lawful search absent the challenged conduct. *United States v. Rosario*, 5 F.4th 706, 713 (7th Cir. 2021); *see also United States v. Alston*, 941 F.3d 132, 138 (4th Cir. 2019) (inevitable discovery requires proof by preponderance that police legally *could* have uncovered the evidence, and that they *would* have done so) (internal citations omitted).

Regarding the first criterion, in both instances that the FBI sought voluntary disclosures from Facebook, the government had sufficient information for a search warrant of the accounts, and the investigation would only go on to develop additional probable cause from independent sources thereafter. In March of 2019, the defendant, who had previously expressed a desire to travel overseas and kill Americans, renewed posting pro-ISIS, violent content on the Carl Johnson Facebook account and connected with like-minded individuals online. The government submits that alone supplies probable cause to search that account. Furthermore, in March 2019,

OCE-3 became Facebook friends with the defendant over the Carl Johnson account and engaged him conversation. Ex. 1 at 11. In June 2019, the defendant discussed with OCE-3 his planning for "an operation" "in this next couple of months." Ex. 5 at 6. Then the defendant's financial records showed him sending thousands of dollars to the aforementioned Philippines-based individual, who was arrested on weapons charges and was publicly linked to ISIS in the news in July 2019. Thus, there is a "clear chain of probable cause, which would have supported warrants had the police applied for them." *Rosario*, 5 F.4th at 713.

Regarding the second prong, after viewing the defendant's extreme, pro-ISIS public content, after seeing him tell OCE-3 that he was planning an operation, and after seeing thousands of dollars transferred to a woman arrested for supplying bomb-making materials to an ISIS cell in the Philippines, the FBI would have clearly sought warrants if not for the voluntary disclosures provided by Facebook in compliance with § 2702. *See Rosario*, 5 F.4th at 714 (government's compliance "with the framework set out in the Stored Communications Act" established that they would undoubtedly have sought a warrant otherwise). And the government did just that in August 2019, applying for and receiving warrants for the content of nine Facebook accounts associated with the defendant, including the two that were the subject of the voluntary disclosure requests. *See United States v. Whitehorn*, 813 F.2d 646, 650 (4th Cir. 1987) (inevitable discovery rule may be applied even though the evidence validly obtained under a search warrant was previously uncovered in an illegal search).

D. If suppression is warranted, it should only be with respect to non-public communications contained in the § 2702 returns.

Should the Court determine that suppression is warranted despite the exigent circumstances, the good faith reliance on the statute, and the inevitable discovery of the materials in question, the government submits that the only thing that need be suppressed is the non-public

information provided by Facebook on March 20, 2019, and August 1, 2019. As noted by defense counsel in their motion, "most federal courts to rule on the issue have agreed that Facebook and other social media users have a reasonable expectation of privacy in content that they *exclude* from public access, such as private messages." *United States v. Zelaya-Veliz*, 94 F.4th 321, 333–34 (4th Cir. 2024) (emphasis added). As a result, the public posts by the Carl Johnson and Al Muzanee accounts that were provided by Facebook on March 20, 2019, and August 1, 2019, should not be suppressed.

Two warrants in this case, one for the defendant's residence (1:19-sw-1102) and one for nine Facebook accounts (1:19-sw-1111), referred to one or both of the § 2702 returns for the Carl Johnson and Al Muzanee accounts.[7] But these search warrants still support a finding of probable cause once any mention of private messages obtained via the § 2702 returns is excised. *See United States v. Gillenwaters*, 890 F.2d 679 (4th Cir. 1989) (finding that excising all information obtained from an illegal search in a subsequent search warrant affidavit is the appropriate remedy); *see also Murray v. United States*, 487 U.S. 533 (1988) ("While the government should not profit from its illegal activity, neither should it be placed in a worse position than it would otherwise have occupied."). For example, in the search warrant for nine social media accounts (including the Carl Johnson and Al Muzanee accounts) issued on August 8, 2019, the accounts are tied to the defendant by subscriber data, IP address information, an OCE, and more. Even ignoring any private information obtained via the § 2702 requests, the affidavit established sufficient probable cause using public posts taken from the Carl Johnson account, Facebook returns obtained from another investigation, conversations with the OCE, and

[7] The other search warrants in this case that included probable cause drawn from content from the Carl Johnson and Al Muzanee accounts occurred after the government obtained the August 8, 2019, warrant for nine social media accounts.

financial records demonstrating that the defendant sent money to two women in the Philippines. As explained in the affidavit, one of these women admitted to the FBI to being an ISIS supporter and to passing some of the money received from the defendant onto her husband, who was an ISIS fighter. Ex. 4, Affidavit at 17. Both of these women were charged with possession of firearms, ammunition and explosives, and purchasing bomb-making materials in the Philippines. The probable cause is similar for the residential search warrant as well. Thus, the government submits there is ample probable cause even without the private communications from the § 2702 returns.

If the Court decides to suppress information that Facebook disclosed pursuant to either or both emergency disclosure requests, the government respectfully requests the opportunity to brief the impact on evidence obtained pursuant to particular warrants in more depth.

CONCLUSION

For the foregoing reasons, the United States respectfully submits that the defendant's motion should be denied.

Respectfully submitted,

Jessica D. Aber
United States Attorney

By: /s/
Anthony T. Aminoff
Amanda St. Cyr
Assistant United States Attorneys
United States Attorney's Office
2100 Jamieson Avenue
Alexandria, VA 22314
Telephone (703) 299-3790
Facsimile (703) 299-3980
Anthony.aminoff@usdoj.gov

Andrew J. Dixon

Andrea Broach
Trial Attorneys
Counterterrorism Section
National Security Division, Dept. of Justice

CERTIFICATE OF SERVICE

I hereby certify that on the 4th day of October, 2024, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system.

/s/

Anthony T. Aminoff
Assistant United States Attorney
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, VA 22314
Telephone (703) 299-3790
Facsimile (703) 299-3980
Anthony.aminoff@usdoj.gov